UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,898	08/28/2006	Kaoru Yokota	2006_1396A	4382

52349 7590 10/12/2010

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
KING, CURTIS J	

ART UNIT	PAPER NUMBER
2612	

NOTIFICATION DATE	DELIVERY MODE
10/12/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ddalecki@wenderoth.com
eoa@wenderoth.com

Office Action Summary	Application No.	Applicant(s)	
	10/590,898	YOKOTA ET AL.	
	Examiner	Art Unit	
	Curtis J. King	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6-8,11,12,22 and 24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6-8,11,12,22 and 24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. Claims 1, 2, 6, 8, 11, 22 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Sukegawa (Pub. No.: US 2003/0039380 A1).

1) In regard to claim 2, Ono discloses the claimed authentication apparatus (Ono fig. 1: 200) which permits a user to use a function provided by the authentication apparatus (Ono fig. 1: 200) if authenticity of the user is certified by authentication (Ono ¶0038 discloses the process unit (fig. 2: 210 which part of the authentication apparatus unit) performs a desired process after the user is authenticated), the authentication apparatus (Ono fig. 1: 200) comprising:

a tag verification information storage unit (Ono fig. 2: 210 discloses as an Authentication Information Holding Unit) operable to store a plurality of pieces of tag verification information (Ono fig. 3: shows a plurality of tag verification information for each article stored in the authentication information holding unit) for identifying a plurality of wireless IC tags respectively (Ono ¶0036 & fig. 3 discloses that a plurality of articles can be received by the authentication apparatus);

a receiving unit (Ono fig. 2: 230 & ¶0037 discloses the personal authentication unit serves also as an authentication information receiving unit) operable to wirelessly receive (Ono ¶0046, 0052 & 0057 discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from wireless IC tags (Ono fig. 1: 102a) attached to objects (Ono fig. 1: 102 discloses as a portable article) carried by the user (Ono ¶0033), a plurality of pieces of tag certification information (Ono ¶0046 discloses that the authentication information transmitted from the IC card and read by radio is identical with the authentication information selected from the authentication information holding unit, hence, it's obvious the IC card has a plurality of pieces of tag certification information) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102) respectively (Ono fig. 3 & ¶0040 discloses the authentication holding unit holds the names of the articles for authentication and the authentication of the IC tags);

a tag judgment unit (Ono integrated in the personal authentication unit; not shown but it's inherent) operable to judge whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition (Ono ¶0046-0047); and

a permission unit (Ono fig. 2: 230 discloses as a processing unit) operable to permit a use of the function if the tag judgment unit (Ono not shown but it's inherent) judges that the level of match satisfies the predetermined condition (Ono ¶0038 discloses the process unit performs a desired process using the individual information of the IC card after the personal authentication unit has certified the right person)

wherein the plurality of pieces of tag verification information are a plurality of verification ID codes (Ono fig. 3: shows that the tag verification information are ID codes (i.e., authentication information & weight coefficients)) for identifying the plurality of wireless IC tags respectively (Ono fig. 3 shows the authentication information (i.e., 1125) stored in the authentication apparatus 200 authentication information holding unit 210 is used to identify the IC tags (i.e., 1125 identifies glasses)),

wherein the plurality of pieces of tag certification information are a plurality of certification ID codes (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, the certification ID codes is disclose as the authentication information & weight coefficients) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects respectively (Ono fig. 3 & ¶0041 it's obvious that the authentication information stored in the tag are codes (i.e., fig. 3: article 1125) that are used to identify the IC tags).

Ono does not disclose the authentication apparatus comprising an identification information storage unit operable to store first identification information, and a user judgment unit operable to, if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information matches the received second identification information, and the permission unit permits the use of the function if the

tag judgment unit judges that the level of match does not satisfy the predetermined condition, and the user judgment unit judges that the first identification information matches the received second identification information, and wherein the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, acquire at least two certification ID codes out of the plurality of certification ID codes received by the receiving unit, and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes.

Sukegawa discloses an authentication apparatus (fig. 16: A5) comprising an identification information storage unit (¶0171 and fig. 19 discloses the authenticator 2 acquires an inputted password from a user to authenticate the user after biometric authentication has failed; not shown, but obvious that the authenticator 2 has an identification information storage unit) operable to store first identification information (¶0171 discloses the unit receives a password from user after the acquired data obtain from the person failed to authenticate the user fig. 19, thus, it is obvious first information is stored), and

a user judgment unit (fig. 19: 2 and ¶0170-0171) operable to judge if the level of match does not satisfy the predetermined condition (¶0170-0171), receive second identification information (¶0171) and judge whether or not the first identification information matches the received second identification information (¶0171 discloses the

unit determines if the password entered (i.e., second identification information) by the person O is used to authenticate the user).

a permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and the user judgment unit judges that the first identification information matches the received second identification information (¶0170-0175, figs. 16 and 19 discloses that the authentication unit allows access if the authenticator determines that the level of match of the first acquired data does not meet a predetermined condition, however, the second entered authentication data (i.e., password) is successfully authenticated; thus, it is obvious that the authentication device has a permission unit that operates as claimed), and

that the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, acquire the data wirelessly received by the receiving unit, and update contents of the dictionary storage unit by storing the acquired data into the dictionary storage unit (¶0170-0175, figs. 16 and 19 discloses that the authentication unit updates the content of the storage device with the acquired data received by the user during step S71; ¶0135 discloses the each user may carry around an IC card (i.e., tag); ¶0138 discloses that the IC card may contain the biometric data used to authenticate a user; ¶0143 discloses that the authenticator may perform authentication by using only the data on the IC card; ¶0145 discloses that the dictionary updating unit updates the dictionary with authentication data acquired from the IC card. Figure 19 shows at step 72 that an authentication credential is received by the

authenticator. Thus, it would have been obvious to one of ordinary skilled in the art that the IC card described in ¶0135-143 may be used to acquire the biometric data for the authentication process as a known alternative way of receiving authentication data wirelessly).

In view of the teachings by Ono and Sukegawa, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement in Ono authentication apparatus a storage unit that stores a password whereby a user is required to enter the correct password as second identification information in order to be granted access by the device if a first authentication process was performed by a first authentication process and failed to match (e.g. because new previously unrecognized authentication credentials are presented), and update the contents of the authentication apparatus with the first authentication data entered during the first authentication process, as taught by Sukegawa for the predictable result of adding an additional feature to the device to allow the user to authenticate him/herself while updating registration of new authorization credentials if the first authentication process fails to authenticate the user.

As to the limitation that a plurality of codes are received an updated: It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made that the combination of Ono and Sukegawa may be used to receive more than one piece of authentication data at the time of a first authentication and update the

authentication apparatus with the received more than one piece of authentication data. The motivation would be since Ono unit may need to receive multiple tag information in order to authenticate a user if the tag combination of the user does not satisfy the authentication apparatus a second authentication process would be done as taught by Sukegawa whereby a user may enter a password to authenticate the user. Thus, if the user is authenticated during the second authentication process the authentication apparatus would update the storage unit with the received tag combination, thereby, allowing the user to access the device next time the user approaches the authentication apparatus with the updated tag combination.

2) In regard to claim 6 (dependent on claim 2), Ono and Sukegawa further discloses the authentication apparatus of claim 2, wherein

the predetermined condition for update is that the first identification information matches the second identification information (Sukegawa ¶0171), and

the update unit updates the contents of the tag verification information storage unit if the first identification information matches the second identification information (Sukegawa ¶0172).

3) In regard to claim 8 (dependent on claim 2), Ono and Sukegawa further discloses the authentication apparatus of claim 2, wherein each of the plurality of certification ID codes (Ono fig. 3: authentication information & weight coefficients) contains a type code (Ono fig. 3: authentication information (e.g., 1125)) indicating a

type of an object to which a wireless IC tag (Ono fig. 1: 102a) identified by the certification ID code is attached (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, it's obvious the authentication information (certification ID codes) contain a type code (glasses) and the authentication information code (i.e.,) corresponds to that article (glasses see fig. 3)), and the update unit (Sukegawa figs. 16 and 19) is further operable to acquire at least two certification ID codes (Sukegawa discloses obtains data for a first authentication process. The same obvious rationale used in claimed 2 that a plurality of codes may be received is being applied to this limitation by the Examiner) containing a predetermined type code (Ono fig. 3: authentication information column shows the predetermined type code for each article), from the plurality of certification ID codes received by the receiving unit (Ono fig. 2: 230).

4) In regard to claim 11 (dependent on claim 8), Ono and Sukegawa further disclose the authentication apparatus of claim 8,

a point storage unit (Ono fig. 3 & ¶0048 integrated into the authentication holding unit discloses as weight coefficient are summed up to authenticate a user) operable to store a plurality of point values (Ono fig. 3: weight coefficient column) with a plurality of type codes (Ono fig. 3: authentication information) corresponding thereto (Ono fig. 3: authentication information column corresponds to the weight coefficient column),

wherein the predetermined type codes (Ono fig. 3: authentication information) are correlated with point values (Ono fig. 3: authentication information column corresponds to the weight coefficient column) that are equal to or higher than a point-value threshold value (Sukegawa ¶0170 discloses the inputted authentication has to meet a predetermined condition), and the update unit is further operable to acquire at least two (Sukegawa discloses obtains data for a first authentication process. The same obvious rationale used in claimed 2 that a plurality of codes may be received is being applied to this limitation by the Examiner) certification ID codes (Ono fig. 3: authentication information & weight coefficients) that have point values (Ono fig. 3: weight coefficient column) that are equal to or higher than the point-value threshold value (Sukegawa ¶0170 discloses the inputted authentication has to meet a predetermined condition), from the plurality of certification ID codes received by the receiving unit (Ono ¶0036), and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority (Sukegawa ¶0170-0175 discloses that the authentication device obtain data for a first authentication process and uses a second authentication process if the first is unsuccessful whereby the authentication device updates the storage unit with the first entered authentication data if the second process is successful. The same obvious rationale used in claimed 2 that a plurality of codes may be received is being applied to this limitation by the Examiner).

5) In regard to claim 1, claim 1 is analyzed and rejected with respect to claim 2.

6) In regard to claim 22, claim 22 is analyzed and rejected with respect to claim 2.

7) In regard to claim 24, claim 24 is directed toward embodying the method of claim 22 in a "computer readable medium".

Ono and Sukegawa does not disclose a computer-readable recording medium recording therein an authentication program that causes a computer to operate as an authentication apparatus which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication.

It would have been obvious to embody the procedures of Ono and Sukegawa discussed with respect to claim 22 in a "computer readable medium" in order that the instructions could be automatically performed by a processor.

3. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Sukegawa (Pub. No.: US 2003/0039380 A1) and further in view of Arens (PG-Pub No. 2001/0030603 A1).

1) In regard to claim 7 (dependent on claim 2), Ono and Sukegawa discloses the authentication apparatus of claim 2.

Ono and Sukegawa do not disclose the authentication apparatus comprises a distance calculating unit operable to measure values of a response time during communication between the authentication apparatus and each of the wireless IC tags

attached to the objects, and calculate values of a distance between the authentication apparatus and each of the wireless IC tags attached to the objects based on the measured values of the response time, wherein the update unit is further operable to acquire at least two certification ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, from the plurality of received certification ID codes.

However, it is well known in the art of location systems that a first device can be determined to exceed a predetermined distance from a second device by measuring the response time of the signals transmitted and determining the distance between the two devices. Arens discloses a location system comprising a distance calculating unit (fig. 7: 70 discloses as a timer) operable to measure values of a response time during communication between the device 2 and device 1 (¶0038), and calculate values of a distance between device 2 and device 1 based on the measured values of the response time (¶0039 discloses the distance is determined (i.e., calculated) by the time recorded by the timer). Arens further discloses that the calculated values of the distance are compared to a predetermined value to see if the two devices are separated by more than the predetermined value (fig. 2: 26 and ¶0024).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement in Ono and Sukegawa authentication apparatus a distance calculating unit, as taught by Arens for the predictable result of alerting a user when he/she is out of the range of a device in which authenticates the user. The combination of Ono, Sukegawa and Ares would yield to the claim limitation "a distance

calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of certification ID codes have been received, wherein the update unit is further operable to acquire at least two certification ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, from the plurality of received certification ID codes (Hence, with the addition of Ares distance calculating unit, Ono and Sukegawa authentication apparatus would obviously be motivated to validate the codes that are determined to be within a certain range which would be done by the update unit, since these are the only codes that the device can be certain are in the proximity of the device)".

The motivation would be to provide an additional feature to the device in which would allow the system to become more secure. For example, if a user leaves the proximity without logging off the authentication device the distance calculating means may insure that the device is shut down and no one can come behind the user and use the device without his/her knowledge.

4. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Sukegawa (Pub. No.: US 2003/0039380 A1) and further in view of Omae (PG-Pub No. 2006/0174121 A1).

1) In regard to claim 12 (dependent on claim 11), Ono and Sukegawa disclose the authentication apparatus of Claim 11.

Ono and Sukegawa do not disclose the authentication apparatus comprises a point update unit operable to receive a type code and a point value, and update the point storage unit by replacing a point value, which is stored in the point storage unit in correspondence with the received type code, with the received point value.

Omae discloses an apparatus that comprises an update unit operable to receive a code (Omae fig. 8: discloses as Device ID/Attribute Setting and Update Unit that is operable to receive a device ID, ¶0069) and update a value (Omae ¶0069 discloses that the Device ID/Attribute Setting and Update Unit can change the value of a device). Although Omae may not disclose his device is used as a point update unit, it would have been obvious to replace Omae update unit in order to update a value of a device, there by increasing the security of the authentication device.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement in Ono and Sukegawa authentication apparatus a update unit to bring up to date the values stored in the device, as taught by Omae. The combination of Ono, Sukegawa and Omae would yield to the claim limitation "a point update unit operable to receive a type code and a point value, and update the point storage unit by replacing a point value, which is stored in the point storage unit in correspondence with the received type code, with the received point value".

The motivation would be to simplify management process of the group management server without reducing the security (Omae ¶0017).

Response to Arguments

Claims 1, 2, 22, and 24

5. Applicant's arguments filed on August, 9, 2010, have been fully considered but they are not deemed persuasive.

As to claims 1, 2, 22, and 24, on page 10 of Applicant's Response, applicant argues:

> **"no disclosure that the dictionary is updated with wirelessly received information from wireless IC tags"**

The Examiner respectfully disagrees with applicant's argument, because Sukegawa ¶0135 discloses that each user may carry around an IC card (i.e., tag); ¶0138 discloses that the IC card may contain the biometric data used to authenticate a user; ¶0143 discloses that the authenticator may perform authentication by using only the data on the IC card; ¶0145 discloses that the dictionary updating unit updates the dictionary with authentication data acquired from the IC card. Figure 19 shows at step 72 that an authentication credential is received by the authenticator. Thus, it would have been obvious to one of ordinary skilled in the art that the IC card described in ¶0135-145 may be used to acquire the biometric data for the authentication process as a known alternative way of receiving authentication data wirelessly and used to update the dictionary information.

Therefore, applicant's argument is not deemed persuasive to overcome the rejection, and the rejection is maintained.

Dependent claims that rely on the arguments of the above claims

6. As to the dependent claims, in which applicant has relied on the arguments of the above argued claims, the above response to the argued claims is the response to the dependent claims.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Curtis J. King whose telephone number is (571)270-5160. The examiner can normally be reached on Mon-Thurs 7:30 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Benjamin C. Lee can be reached on (571)272-2963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ck/

/BENJAMIN C. LEE/
Supervisory Patent Examiner, Art Unit 2612